Higher Weights for Codes over Finite Rings (Codes, lattices, vertex operator algebras and finite groups)

AUTHOR(S):

Horimoto, Hiroshi; Shiromoto, Keisuke

CITATION:

Horimoto, Hiroshi ...[et al]. Higher Weights for Codes over Finite Rings (Codes, lattices, vertex operator algebras and finite groups). 数理解析研究所講究録 2001, 1228: 28-34

ISSUE DATE:

2001-09

URL:

http://hdl.handle.net/2433/41421

数理解析研究所講究録 1228 巻 2001 年 28-34

Higher Weights for Codes over Finite Rings

Hiroshi Horimoto (堀本 博)
and
Keisuke Shiromoto (城本 啓介)*
Department of Mathematics, Kumamoto University
(熊本大学理学部数理科学科)

1 Introduction

For an $[n, k]$ code C over a finite field $\mathbb{F}_q$ and $1 \leq r \leq k$, the rth *generalized Hamming weight* (GHW) $d_r(C)$ of C is defined by Wei ([10]) as follows:

$$d_r(C) := \min\{|\mathrm{Supp}(D)| : \ D \text{ is a } [n, r] \text{ subcode of } C\},$$

where $\mathrm{Supp}(D) := \cup_{\boldsymbol{x} \in D} \mathrm{supp}(\boldsymbol{x})$ and $\mathrm{supp}(\boldsymbol{x}) := \{i \mid x_i \neq 0\}$ for $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$. A lot of papers dealing with GHW for codes over finite fields have been published (see [9] etc.).

On the other hand, in the last few years, linear codes over finite rings have been in the focus of the coding research (see [3], [5], [6], [7] and [11], etc.). In particular, Ashikhmin, Yang, Helleseth *et al.* ([1], [12], [13] and [4]) introduced the rth *generalized Hamming weight with respect to order* (GHWO) $d_r(C)$ for a linear code C of length n over $\mathbb{Z}_4$ and $1 \leq r \leq \log_4 |C|$ as follows:

$$d_r(C) := \min\{|\mathrm{Supp}(D)| : \ D \text{ is a submodule of } C \text{ with } \log_4 |D| = r\}.$$

And they exactly determined $d_r(C)$ of Preparata, Kerdock, Goethals codes *et al.* over $\mathbb{Z}_4$ for some r.

In this paper, we shall introduce a concept of *rank* for linear codes over finite chain rings and consider some fundamental properties of a generalized Hamming weight with respect to rank for these codes.

In this paper, all rings are assumed to be finite and associative with $1 \neq 0$. In any module, 1 is assumed to act as the identity.

*Research Fellow of the Japan Society for the Promotion of Science.

2 Codes over Finite Chain Rings.

A finite ring R with Jacobson radical $J(R) \neq 0$ is call as a *chain ring* if the principal left ideals of R form a chain (see [8] and [5]). We remark that a finite chain ring R can be viewed as a local ring with $J(R) = R\theta$ for any $\theta \in J(R)\backslash J(R)^2$. For example, the ring $\mathbb{Z}/q\mathbb{Z}$ of integers module q, where q is a prime power, the Galois ring $GR(q,m)$ of characteristic q with q^m elements and $\mathbb{F}_2 + u\mathbb{F}_2$ $(u^2 = 0)$ are chain rings. On the other hand, $\mathbb{Z}/k\mathbb{Z}$, where k is not a prime power, and $\mathbb{F}_2 + v\mathbb{F}_2$ $(v^2 = v)$ are not chain rings. Let m be the index of nilpotency of $J(R)$ and let R^* be the group of units of R. In addition, since R is a local ring, we denote by a prime power q the cardinality of the finite field $R/J(R)$, that is, $R/J(R) \cong \mathbb{F}_q$ and $|R| = q^m$. Let R^n be the free R-module of rank n consisting of all n-tuples of elements of R. With respect to component-wise addition and right/left multiplication, R^n has the structure of an (R,R)-bimodule. A *right* (resp., *left*) *linear code* C of length n over R is a right (resp., left) R-submodule of R^n. If C is a free R-submodule of R^n, then we shall call C as a *free code*. For a right (left) linear code C over R, we define the rank of C, denoted by rank(C), as the minimum number of generators of C and define the *free rank* of C, denoted by f-rank(C), as the maximum rank of the free R-submodules of C. In this case, C is isomorphic, as an R-module, to a direct sum:

$$C \cong \bigoplus_{i=1}^{m} (R/R\theta^i)^{k_i},$$

where $R\theta^i := \{r\theta^i \mid r \in R\} = \{x \in R \mid x\theta^{m-i} = 0\}$, for each $i \in \{1,2,\ldots,m\}$. We note that rank$(C) = \sum_{i=1}^{m} k_i$ and f-rank$(C) = k_m$, and define the *type* of C, denoted by type(C), as the sequence $(k_1, k_2, \ldots, k_m)$. For an R-module M, the *socle* of M, that is, the sum of all simple submodules of M, is denoted by Soc(M). For a right (resp., left) linear code C over R, we note that

$$\mathrm{Soc}(C) = \{\boldsymbol{x} \in C \mid \boldsymbol{x}\theta = \boldsymbol{0}\}$$
$$(\text{resp., } \mathrm{Soc}(C) = \{\boldsymbol{x} \in C \mid \theta\boldsymbol{x} = \boldsymbol{0}\}).$$

For a right (left) linear code C over R, we define $I(C)$ as a minimal free R-submodule of R^n which contains C and define $F(C)$ as a maximal free R-submodule of C. If C is a right (resp., left) linear code of length n over R, then $I(C)$ is a right (resp., left) free code of length n with rank$(I(C))$ = rank(C) and $F(C)$ is a right (resp., left) free code of length n with rank$(F(C))$ = f-rank(C) (cf. [7]).

For a vector $\boldsymbol{x} = (x_1, \ldots, x_n) \in R^n$, the *support* of $\boldsymbol{x}$ is defined by

$$\mathrm{supp}(\boldsymbol{x}) := \{i \mid x_i \neq 0\}$$

and the *Hamming weight* $\mathrm{wt}(\boldsymbol{x})$ of $\boldsymbol{x}$ is defined to be the order of the support of $\boldsymbol{x}$. The *minimum Hamming weight* of a linear code C of length n over R is

$$d(C) := \min\{\mathrm{wt}(\boldsymbol{x}) \mid (\boldsymbol{0} \neq)\boldsymbol{x} \in C\}.$$

If $\mathrm{Soc}(R) \cong R/J(R)$ as right R-modules and as left R-modules, then R is called as a *Frobenius ring* ([8], [7] and [11]). Since a chain ring R is a Frobenius ring, we have an R-isomorphism $\phi : \mathrm{Soc}(R) \cong R/J(R)$. In this case, ϕ induces the following R-isomorphism:

$$\begin{aligned} \phi^n &: \mathrm{Soc}(R)^n \cong (R/J(R))^n \\ &: \boldsymbol{x} = (x_1, \ldots, x_n) \mapsto \phi^n(\boldsymbol{x}) = (\phi(x_1), \ldots, \phi(x_n)), \end{aligned}$$

(cf. [8] and [7]). We have the following proposition.

Proposition 2.1 ([7]) *If C is a right (left) linear code of length n over R, then $\phi^n(\mathrm{Soc}(C))$ is a linear $[n, \mathrm{rank}(C), d(C)]$ code over the finite field $R/J(R)$.*

For two vectors $\boldsymbol{x} = (x_1, \ldots, x_n) \in R^n$ and $\boldsymbol{y} = (y_1, \ldots, y_n) \in R^n$, we define the *inner product*

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle := x_1 y_n + \cdots + x_n y_n.$$

For a subset $C \subseteq R^n$, we define the *right dual code* $C^\perp$ and the *left dual code* ${}^\perp C$ of C as follows:

$$\begin{aligned} C^\perp &:= \{\boldsymbol{y} \in R^n \mid \langle \boldsymbol{x}, \boldsymbol{y} \rangle = 0, \ \forall \boldsymbol{x} \in C\} \\ {}^\perp C &:= \{\boldsymbol{y} \in R^n \mid \langle \boldsymbol{y}, \boldsymbol{x} \rangle = 0, \ \forall \boldsymbol{x} \in C\}. \end{aligned}$$

If C is a right (resp., left) linear code of length n over R, then

$$\begin{gathered} \mathrm{rank}(C) + \text{f-rank}({}^\perp C) = n \\ (\text{resp., } \mathrm{rank}(C) + \text{f-rank}(C^\perp) = n) \end{gathered}$$

and $({}^\perp C)^\perp = C$ (resp., ${}^\perp(C^\perp) = C$) (cf. [5] and [7]).

A generator matrix of a right (resp., left) linear code C of length n over R is a $\mathrm{rank}(C) \times n$ matrix over R whose rows form a minimal set of generators of C. Similarly, a *parity check matrix* of C is an $n \times (n - \text{f-rank}(C))$ matrix over R whose columns form a minimal set of generators of ${}^\perp C$ (resp., $C^\perp$).

In the remaining part of this paper, we shall concentrate on right linear codes because all results and proofs for left linear codes always go through as well as those for right linear codes.

3 Generalized Hamming Weights

For a subset $C \subseteq R^n$, we define the *support* of C by

$$\mathrm{Supp}(C) := \bigcup_{\boldsymbol{x} \in C} \mathrm{supp}(\boldsymbol{x}).$$

Evidently we note that if C_1 and C_2 are subsets of R^n such that $C_1 \subseteq C_2$, then $|\mathrm{Supp}(C_1)| \leq |\mathrm{Supp}(C_2)|$.

Definition 3.1 For a right linear code C of length n over R and $1 \leq r \leq \mathrm{rank}(C)$, the rth *generalized Hamming weight with respect to rank* (GHWR) of C is defined by

$$d_r(C) := \min\{|\mathrm{Supp}(D)| : \ D \text{ is an } R\text{-submodule of } C \text{ with } \mathrm{rank}(D) = r\}.$$

The *weight hierarchy* of C is the set of integers $\{d_r(C) : \ 1 \leq r \leq \mathrm{rank}(C)\}$

The following lemma is essential.

Lemma 3.2 *If C is a right (left) linear code of length n over R, then*

$$\mathrm{Soc}(C) = \mathrm{Soc}(I(C)).$$

The following result is a generalization of Proposition 2.1 with respect to GHWR.

Theorem 3.3 *Let C be a right linear code C of length n over R. Then*

$$d_r(C) = d_r(\mathrm{Soc}(C)) = d_r(I(C)),$$

for any r, $1 \leq r \leq \mathrm{rank}(C)$.

Remark 3.4 The above theorem also claims that all free R-submodules of R^n which contain C and have the same rank as C have the same weight hierarchy as C.

Using the above theorem, we have the following results from Theorem 1 and Corollary 1 in [10].

Corollary 3.5 *For a right linear code C of length n over R with* $\mathrm{rank}(C) = k > 0$,

$$1 \leq d_1(C) < d_2(C) < \cdots < d_k(C) \leq n.$$

Corollary 3.6 *For a right linear code C of length n over R and any r, $1 \leq r \leq \mathrm{rank}(C)$,*

$$d_r(C) \leq n - \mathrm{rank}(C) + r.$$

If C meets the above bound, i.e., $d_r(C) = n - \mathrm{rank}(C) + r$, then C is called an rth *MDS code* over R. In [2] and [7], the first MDS codes over the finite rings (simply called MDR or MDS codes in these papers) are studied.

For a right linear code C of length n and $M \subseteq N := \{1, 2, \ldots, n\}$, we set

$$\begin{aligned} R^n(M) &:= \{\boldsymbol{x} \in R^n \mid \mathrm{supp}(\boldsymbol{x}) \subseteq M\} \\ C(M) &:= C \cap R^n(M) = \{\boldsymbol{x} \in C \mid \mathrm{supp}(\boldsymbol{x}) \subseteq M\}. \end{aligned}$$

Clearly, $R^n(M)$ is a free R-module of rank $|M|$ and $C(M)$ is also a right linear code of length n over R. And for right linear codes C and D over R and a linear map $\psi : C \to D$, we define

$$\begin{aligned} C^* &:= \mathrm{Hom}_R(C, R) \\ \psi^* &: D^* \to C^* \\ &: g \mapsto g\psi. \end{aligned}$$

Moreover, there is the following isomorphism as left R-modules:

$$\begin{aligned} f &: R^n \to (R^n)^* \\ &: \boldsymbol{x} \mapsto (f(\boldsymbol{x}) : \boldsymbol{y} \mapsto \langle \boldsymbol{x}, \boldsymbol{y} \rangle). \end{aligned}$$

Then the following proposition is essential.

Proposition 3.7 ([6]) *Let C be a right linear code of length n over R. Then the sequence*

$$0 \longrightarrow {}^{\perp}C(N - M) \xrightarrow{\mathrm{inc}} R^n(N - M) \xrightarrow{f} C^* \xrightarrow{\mathrm{res}} C(M)^* \longrightarrow 0$$

is exact as left R-modules for any $M \subseteq N$, where the maps inc, res *denote the inclusion map, the restriction map, respectively.*

In [6], they proved the Singleton type bound for codes over finite quasi-Frobenius rings by using this proposition. In this paper, we prove a duality for GHWR of codes over finite chain rings using this proposition.

Lemma 3.8 *Let C be a right linear code of length n over R. Then*

$$d_r(C) = \min\{|M| : \ \mathrm{rank}(C(M)) = r, \ M \subseteq N\},$$

for all r, $1 \leq r \leq \mathrm{rank}(C)$.

A duality for GHW of codes over finite fields is proved in [10] and similarly, a duality for GHWO of codes over Galois rings is proved in [1]. As in these case, we have a similar duality relation for GHWR of codes over finite chain rings as follows:

Theorem 3.9 *Let C be a right linear code of length n over R with* $\mathrm{rank}(C) = k$. *Then*

$$\{d_r(C) : \ 1 \le r \le k\} = \{1, 2, \ldots, n\} \backslash \{n + 1 - d_r(F(^{\perp}C)) : \ 1 \le r \le n - k\}.$$

Though we have many possibilities of taking $F(C)$ for a right linear code C, the following result follows from the above theorem.

Corollary 3.10 *If C is a right linear code of length n over R with* $\text{f-rank}(C) = k_0$, *then all right free R-submodules of C with rank k_0 have the same weight hierarchy determined by that of $^{\perp}C$.*

Now we introduce a weight for a vector in R^n which is a generalization of the Lee weight for a vector in $\mathbb{Z}_4^n$. For an element $(0 \neq) x \in R$, we define the *socle weight* $s(x)$ of $(0 \neq) x \in R$ as follows:

$$s(x) = \begin{cases} q - 1 & (x \notin \mathrm{Soc}(R)) \\ q & (x \in \mathrm{Soc}(R)) \end{cases},$$

and set $s(0) = 0$. For example, if $R = \mathbb{Z}_{27} = \{0, 1, 2, \ldots, 26\}$, then $s(x) = 2$ for $x \neq 0, 9, 18$ and $s(x) = 3$ for $x = 9, 18$. For a vector $\boldsymbol{x} = (x_1, \ldots, x_n) \in R^n$, the *socle weight* $w_S(\boldsymbol{x})$ of $\boldsymbol{x}$ is defined by

$$w_S(\boldsymbol{x}) := \sum_{j=1}^{n} s(x_j).$$

For a right linear code C of length n over R, the *minimum socle weight* $d_S(C)$ of C is defined as follows:

$$d_S(C) := \min\{w_S(\boldsymbol{x}) \mid (\boldsymbol{0} \neq) \boldsymbol{x} \in C\}.$$

Lemma 3.11 *Let C be a right linear code of length n and of rank k over R and let A be the $|C| \times n$ array of all codewords in C. Then each column of A corresponds to the following case: the column contains all elements of $R\theta^i$ equally often for any $i \in \{0, 1, \ldots, m-1\}$.*

Then we have the following theorem. A similar result for Lee weights of codes over $\mathbb{Z}_4$ can be found in [12] and corresponds to the special case $R = \mathbb{Z}_4$ in the following result.

Theorem 3.12 *Let C be a right linear code of length n over R. Then we have*

$$|\mathrm{Supp}(C)| = \frac{1}{|C|(q-1)} \sum_{\boldsymbol{x} \in C} w_S(\boldsymbol{x}).$$

Corollary 3.13 *If C be a right linear code of length n over R, then the rth GHWR of C, $1 \le r \le \mathrm{rank}(C)$, satisfies*

$$d_r(C) \ge \left\lceil \frac{(q^r - 1) d_S(C)}{q^r (q-1)} \right\rceil,$$

where $\lceil a \rceil$ denotes the smallest integer greater than or equal to a.

References

[1] A. Ashikhmin, On generalized Hamming weights for Galois ring linear codes, *Designs, Codes and Cryptography*, **14** (1998) pp. 107–126.

[2] S. T. Dougherty and K. Shiromoto, MDR codes over $\mathbb{Z}_k$, *IEEE Trans. Inform. Theory*, **46** (2000) pp. 265–269.

[3] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane and P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Inform. Theory*, **40** (1994) pp. 301–319.

[4] T. Helleseth and K. Yang, Further results on generalized Hamming weights for Goethals and Preparata codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory*, **45** (1999) pp. 1255–1258.

[5] T. Honold and I. Landjev, Linear codes over finite chain rings, *Electronic Journal of Combinatorics*, **7** (2000), no. 1, Research Paper 11.

[6] H. Horimoto and K. Shiromoto, A Singleton bound for linear codes over quasi-Frobenius rings, *Proceedings of the 13th Applied Algebra, Algebraic Algorithms and Error-Correcting Codes* (Hawaii, 1999).

[7] H. Horimoto and K. Shiromoto, MDS codes over finite quasi-Frobenius rings, submitted.

[8] B. R. McDonald, *Finite rings with identity, Pure and Applied Mathematics*, **28** Marcel Dekker, Inc., New York, 1974.

[9] M. A. Tsfasman and S. G. Vladut, Geometric approach to higher weights, *IEEE Trans. Inform. Theory*, **41** (1995) pp. 1564–1588.

[10] V. K. Wei, Generalized Hamming weights for linear codes, *IEEE Trans. Inform. Theory*, **37** (1991)pp. 1412–1418.

[11] J. A. Wood, Duality for modules over finite rings and applications to coding theory, *American journal of Mathematics*, **121** (1999), 555–575.

[12] K. Yang, T. Helleseth, P. V. Kumar and A. G. Shanbhang, On the weights hierarchy of Kardock codes over $\mathbb{Z}_4$. *IEEE Trans. Inform. Theory*, **42** (1996) pp. 1587–1593.

[13] K. Yang and T. Helleseth, On the weight hierarchy of Preparata codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory*, **43** (1997) pp. 1832–1842.